Formal Reasoning for Quantum Programs

Yuxin Deng

East China Normal University

Thanks to Yuan Feng and Mingsheng Ying

Outline

Background

Preliminaries on quantum mechanics

Equivalences for quantum processes

Symbolic semantics

An algorithm for ground bisimulation

Hoare logic

Summary

Outline

Background

Preliminaries on quantum mechanics

Equivalences for quantum processes

Symbolic semantics

An algorithm for ground bisimulation

Hoare logic

Summary

Quantum communication

- In 1984, C. Bennett (IBM) and C. Brassard (Univ. of Montreal) proposed the first protocol for quantum key distribution, the BB84 protocol.

  ⋮

Quantum communication

- In 1984, C. Bennett (IBM) and C. Brassard (Univ. of Montreal) proposed the first protocol for quantum key distribution, the BB84 protocol.

  ⋮

- On August 16, 2016, China launched the first satellite using quantum technology to send communications back to earth.

Quantum communication

- In 1984, C. Bennett (IBM) and C. Brassard (Univ. of Montreal) proposed the first protocol for quantum key distribution, the BB84 protocol.

  ⋮

- On August 16, 2016, China launched the first satellite using quantum technology to send communications back to earth.
- A 2000-km quantum communication main network between Beijing and Shanghai will be fully operational later this year.

Quantum computation

- In 1982, R. Feynman proposed the idea to construct quantum computers based on the theory of quantum mechanics.

  ⋮

Quantum computation

- In 1982, R. Feynman proposed the idea to construct quantum computers based on the theory of quantum mechanics.

  ⋮

- In 2011, the Canadian company D-Wave Systems claimed to have created the first commercial 128-qubit quantum computer, D-wave One.

Quantum computation

- In 1982, R. Feynman proposed the idea to construct quantum computers based on the theory of quantum mechanics.

  $\vdots$

- In 2011, the Canadian company D-Wave Systems claimed to have created the first commercial 128-qubit quantum computer, D-wave One.
- In December 2015, Google announced that, in solving a specific optimization problem, their 512-qubit D-Wave 2X is 100 million times faster than conventional single-core computers.

Quantum programming

"the real challenge will be the software .... Programming this thing [D-Wave] is ridiculously hard; it can take months to work out how to phrase a problem so that the computer can understand it."

— G. Rose
Founder and CTO at D-Wave Systems

[N. Jones. The Quantum Company. *Nature* 498:286-288, 2013.]

Quantum programming languages

- "Quantum data, classical control" [Selinger]
- Sequential languages
  - Quipper [Dalhousie Univ.]
  - LIQUi$|>$ [Microsoft]
  - Scaffold [Princeton]
  - ...

Quantum programming languages

- "Quantum data, classical control" [Selinger]
- Sequential languages
  - Quipper [Dalhousie Univ.]
  - LIQUi$|>$ [Microsoft]
  - Scaffold [Princeton]
  - ...
- Concurrent languages (quantum process algebras) Aiming to specify and verify quantum protocols.
  - QPAlg [Jorrand and Lalire]
  - CQP [Gay and Nagarajan]
  - qCCS [Feng et al.]

In this talk, we focus on

In this talk, we focus on

- Coinduction for quantum processes

In this talk, we focus on

- Coinduction for quantum processes
- Hoare logic for quantum programs

Outline

Background

Preliminaries on quantum mechanics

Equivalences for quantum processes

Symbolic semantics

An algorithm for ground bisimulation

Hoare logic

Summary

Dirac-notation

Let $\mathcal{H}$ be a Hilbert space.

Dirac-notation

Let $\mathcal{H}$ be a Hilbert space.

- 'ket' $|\psi\rangle$ stands for a (normalized) vector in $\mathcal{H}$.

Dirac-notation

Let $\mathcal{H}$ be a Hilbert space.

- 'ket' $|\psi\rangle$ stands for a (normalized) vector in $\mathcal{H}$.
- 'bra' $\langle\psi|$ stands for the adjoint (dual vector) of $|\psi\rangle$.

Dirac-notation

Let $\mathcal{H}$ be a Hilbert space.

- 'ket' $|\psi\rangle$ stands for a (normalized) vector in $\mathcal{H}$.
- 'bra' $\langle\psi|$ stands for the adjoint (dual vector) of $|\psi\rangle$.
- Generally, $A^\dagger$ stands for the adjoint of A, such that

$$(A^\dagger|\psi\rangle, |\phi\rangle) = (|\psi\rangle, A|\phi\rangle).$$

In particular, $(|\psi\rangle)^\dagger = \langle\psi|$.

Quantum states

- Associated to any quantum system is a Hilbert space known as the state space.

Quantum states

- Associated to any quantum system is a Hilbert space known as the state space.
- The state of a closed quantum system is described by a unit vector, say $|\psi\rangle$, in its state space.

Quantum states(Cont'd)

- $\rho = \sum_k p_k |\psi_k\rangle\langle\psi_k|$: lies in the state $|\psi_k\rangle$ with probability p_k, $\sum_k p_k = 1$.
  - ρ is a positive operator
  - $\mathrm{tr}(\rho) = 1$

Quantum states(Cont'd)

- $\rho = \sum_k p_k |\psi_k\rangle\langle\psi_k|$: lies in the state $|\psi_k\rangle$ with probability p_k, $\sum_k p_k = 1$.
  - ρ is a positive operator
  - $\mathrm{tr}(\rho) = 1$
- These two conditions characterize exactly the set of density operators.

Quantum dynamics

A super-operator $\mathcal{E}$ over Hilbert space $\mathcal{H}$ is a linear map on the space of linear operators on $\mathcal{H}$.

Quantum dynamics

A super-operator $\mathcal{E}$ over Hilbert space $\mathcal{H}$ is a linear map on the space of linear operators on $\mathcal{H}$.

- $\mathcal{E}$ is trace-preserving, if $\mathrm{tr}(\mathcal{E}(A)) = \mathrm{tr}(A)$ for any positive operator A.

Quantum dynamics

A super-operator $\mathcal{E}$ over Hilbert space $\mathcal{H}$ is a linear map on the space of linear operators on $\mathcal{H}$.

- $\mathcal{E}$ is trace-preserving, if $\mathrm{tr}(\mathcal{E}(A)) = \mathrm{tr}(A)$ for any positive operator A.
- $\mathcal{E}$ is completely positive, if for any auxiliary space $\mathcal{H}'$ and any positive operator σ on the tensor Hilbert space $\mathcal{H}' \otimes \mathcal{H}$, $(\mathcal{I}_{\mathcal{H}'} \otimes \mathcal{E})(\sigma)$ is also a positive operator on $\mathcal{H}' \otimes \mathcal{H}$.

Quantum dynamics

- The evolution of a quantum system is described by a super-operator

$$\rho' = \mathcal{E}(\rho)$$

Quantum measurements

- An observable A is a Hermitian operator, $A^\dagger = A$. Let

$$A = \sum_k \lambda_k P_k,$$

where P_k is the eigenspace associated with λ_k.

Quantum measurements

- An observable A is a Hermitian operator, $A^\dagger = A$. Let
$$A = \sum_k \lambda_k P_k,$$
where P_k is the eigenspace associated with λ_k.
- If we measure ρ by the observable A, then we obtain the result k with probability
$$p_k = \mathrm{tr}(P_k \rho)$$

Quantum measurements

- An observable A is a Hermitian operator, $A^\dagger = A$. Let

$$A = \sum_k \lambda_k P_k,$$

where P_k is the eigenspace associated with λ_k.

- If we measure ρ by the observable A, then we obtain the result k with probability

$$p_k = \mathrm{tr}(P_k \rho)$$

Quantum measurements

- An observable A is a Hermitian operator, $A^\dagger = A$. Let

$$A = \sum_k \lambda_k P_k,$$

where P_k is the eigenspace associated with λ_k.

- If we measure ρ by the observable A, then we obtain the result k with probability

$$p_k = \mathrm{tr}(P_k \rho)$$

- The measurement disturbs the system, leaving it in a state $P_k \rho P_k / p_k$ determined by the outcome.

Syntax of qCCS

The syntax of qCCS:

$$\mathbf{nil} \mid pref.P \mid P + Q \mid P \| Q \mid P \backslash L \mid \mathbf{if}\ b\ \mathbf{then}\ P \mid A(\tilde{q}; \tilde{x})$$

where

$$pref ::= \tau \mid c?x \mid c!e \mid \underline{c}?q \mid \underline{c}!q \mid \mathcal{E}[\widetilde{q}] \mid M[\widetilde{q}; x]$$

Further requirements

- $c?x.d!x.d!x.0$

$\not\Rightarrow$ $\underline{c}?r.\underline{d}!r.\underline{d}!r.0$

- Quantum no-cloning theorem!

Syntax of qCCS, cont'd

For a process to be legal, we require

1. $q \notin qv(P)$ in the process $\underline{c}!q.P$;
2. $qv(P) \cap qv(Q) = \emptyset$ in the process $P \,||\, Q$.

Operational Semantics of qCCS

A pair of the form

$$\langle P, \rho \rangle$$

is a configuration, where P is a closed quantum process and ρ is a density operator. The set of configurations is denoted by Con. We let $\mathcal{C}, \mathcal{D}, \ldots$ range over Con.

Operational Semantics of qCCS

Let

$$\begin{aligned} Act &= \{\tau\} \cup \{c?v, c!v \mid c \text{ classical channel}, v \text{ real number}\} \cup \\ &\quad \{\underline{c}?r, \underline{c}!r \mid \underline{c} \text{ quantum channel}, r \text{ quantum variable}\}, \end{aligned}$$

and $D(Con)$ be the set of finite-support probability distributions over Con.

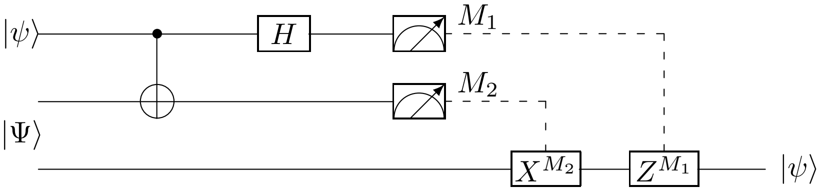
The semantics of qCCS is given by the probabilistic labeled transition system $(Con, Act, \rightarrow)$, where $\rightarrow \subseteq Con \times Act \times D(Con)$ is the smallest relation satisfying some rules.

An example: Teleportation

Quantum teleportation [Bennett, Brassard, Crepeau, Jozsa, Peres, and Wootters, PRL 1993] makes use of a maximally entangled state to teleport an unknown quantum state by sending only *classical* information.

It serves as a key ingredient in many other quantum communication protocols.

An example: Teleportation



Let

$$
\begin{aligned}
Alice &:= CNot[q, q_1].H[q].M[q, q_1; x].c!x.\mathbf{nil} \\
Bob &:= c?x.U_x[q_2].\mathbf{nil} \\
Telep &:= (Alice \| Bob) \backslash \{c\}
\end{aligned}
$$

Here $M = \sum_{i=0}^{3} \lambda_i |\tilde{i}\rangle\langle\tilde{i}|$, and

$$
\begin{aligned}
U_x[q_2].\mathbf{nil} \; &:= \; \mathbf{if}\ x = \lambda_0\ \mathbf{then}\ \sigma_0[q_2].\mathbf{nil} + \mathbf{if}\ x = \lambda_1\ \mathbf{then}\ \sigma_1[q_2].\mathbf{nil} \\
&+ \; \mathbf{if}\ x = \lambda_2\ \mathbf{then}\ \sigma_3[q_2].\mathbf{nil} + \mathbf{if}\ x = \lambda_3\ \mathbf{then}\ \sigma_2[q_2].\mathbf{nil}.
\end{aligned}
$$

$$\langle Telep,\ [(\alpha|0\rangle + \beta|1\rangle) \otimes \tfrac{1}{\sqrt{2}}(|00\rangle + |11\rangle)]\rangle$$

$$\big\downarrow \tau$$

$$\langle (H[q].M[q,q_1;x].c!x.\mathbf{nil} \| Bob)\backslash\{c\},\ [\tfrac{1}{\sqrt{2}}(\alpha(|000\rangle + |011\rangle) + \beta(|110\rangle + |101\rangle))]\rangle$$

$$\big\downarrow \tau$$

$$\langle (M[q,q_1;x].c!x.\mathbf{nil} \| Bob)\backslash\{c\},\ [\tfrac{1}{2}(\alpha(|000\rangle + |100\rangle + |011\rangle + |111\rangle) + \beta(|010\rangle - |110\rangle + |001\rangle - |101\rangle))]\rangle$$

$$\big\downarrow \tau$$

$$\bullet \xrightarrow{1/4} \langle (c!\lambda_0.\mathbf{nil} \| Bob)\backslash\{c\},\ [\alpha|000\rangle + \beta|001\rangle]\rangle \xrightarrow{\tau} \langle (\mathbf{nil} \| \sigma_0[q_2].\mathbf{nil})\backslash\{c\},\ [|00\rangle \otimes (\alpha|0\rangle + \beta|1\rangle)]\rangle \xrightarrow{\tau} \langle (\mathbf{nil} \| \mathbf{nil})\backslash\{c\},\ [|00\rangle \otimes (\alpha|0\rangle + \beta|1\rangle)]\rangle$$

$$\bullet \xrightarrow{1/4} \langle (c!\lambda_1.\mathbf{nil} \| Bob)\backslash\{c\},\ [\alpha|011\rangle + \beta|010\rangle]\rangle \xrightarrow{\tau} \langle (\mathbf{nil} \| \sigma_1[q_2].\mathbf{nil})\backslash\{c\},\ [|01\rangle \otimes (\alpha|1\rangle + \beta|0\rangle)]\rangle \xrightarrow{\tau} \langle (\mathbf{nil} \| \mathbf{nil})\backslash\{c\},\ [|01\rangle \otimes (\alpha|0\rangle + \beta|1\rangle)]\rangle$$

$$\bullet \xrightarrow{1/4} \langle (c!\lambda_2.\mathbf{nil} \| Bob)\backslash\{c\},\ [\alpha|100\rangle - \beta|101\rangle]\rangle \xrightarrow{\tau} \langle (\mathbf{nil} \| \sigma_3[q_2].\mathbf{nil})\backslash\{c\},\ [|10\rangle \otimes (\alpha|0\rangle - \beta|1\rangle)]\rangle \xrightarrow{\tau} \langle (\mathbf{nil} \| \mathbf{nil})\backslash\{c\},\ [|10\rangle \otimes (\alpha|0\rangle + \beta|1\rangle)]\rangle$$

$$\bullet \xrightarrow{1/4} \langle (c!\lambda_3.\mathbf{nil} \| Bob)\backslash\{c\},\ [\alpha|111\rangle - \beta|110\rangle]\rangle \xrightarrow{\tau} \langle (\mathbf{nil} \| \sigma_2[q_2].\mathbf{nil})\backslash\{c\},\ [|11\rangle \otimes (\alpha|1\rangle - \beta|0\rangle)]\rangle \xrightarrow{\tau} \langle (\mathbf{nil} \| \mathbf{nil})\backslash\{c\},\ [|11\rangle \otimes (\alpha|0\rangle + \beta|1\rangle)]\rangle$$

Outline

Background

Preliminaries on quantum mechanics

Equivalences for quantum processes

Symbolic semantics

An algorithm for ground bisimulation

Hoare logic

Summary

Lifted relation

Lift $\mathcal{R} \subseteq S \times S$ to $\mathcal{R}^\circ \subseteq Dist(S) \times Dist(S)$:

Lifted relation

Lift $\mathcal{R} \subseteq S \times S$ to $\mathcal{R}^\circ \subseteq Dist(S) \times Dist(S)$:

1. $s \mathcal{R} t$ implies $\overline{s}\ \mathcal{R}^\circ\ \overline{t}$;

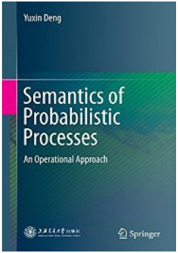
Lifted relation

Lift $\mathcal{R} \subseteq S \times S$ to $\mathcal{R}^\circ \subseteq \mathit{Dist}(S) \times \mathit{Dist}(S)$:

1. $s \mathcal{R} t$ implies $\overline{s}\ \mathcal{R}^\circ\ \overline{t}$;
2. $\Delta_i\ \mathcal{R}^\circ\ \Theta_i$ for all $i \in I$ implies $(\sum_{i \in I} p_i \cdot \Delta_i)\ \mathcal{R}^\circ\ (\sum_{i \in I} p_i \cdot \Theta_i)$ for any $p_i \in [0, 1]$ with $\sum_{i \in I} p_i = 1$, where I is a countable index set.

There are alternative formulations; related to the Kantorovich metric and the network flow problem. See e.g.

http://www.springer.com/978-3-662-45197-7



Four criteria to judge equivalence

A relation $\mathcal{R}$ is

Four criteria to judge equivalence

A relation $\mathcal{R}$ is

- barb-preserving if $\mathcal{C}\mathcal{R}\mathcal{D}$ implies that $\mathcal{C}\Downarrow_c^{\geq p}$ iff $\mathcal{D}\Downarrow_c^{\geq p}$ for any $p \in [0,1]$ and any classical channel c, where $\mathcal{C}\Downarrow_c^{\geq p}$ holds if $\mathcal{C} \stackrel{\hat{\tau}}{\Longrightarrow} \Delta$ for some Δ with

$$\sum\{\Delta(\mathcal{C}') \mid \mathcal{C}' \xrightarrow{c!v} \text{ for some } v\} \ \geq \ p;$$

Four criteria to judge equivalence

A relation $\mathcal{R}$ is

- barb-preserving if $\mathcal{C} \mathcal{R} \mathcal{D}$ implies that $\mathcal{C} \Downarrow_c^{\geq p}$ iff $\mathcal{D} \Downarrow_c^{\geq p}$ for any $p \in [0, 1]$ and any classical channel c, where $\mathcal{C} \Downarrow_c^{\geq p}$ holds if $\mathcal{C} \stackrel{\hat{\tau}}{\Longrightarrow} \Delta$ for some Δ with

$$\sum \{ \Delta(\mathcal{C}') \mid \mathcal{C}' \xrightarrow{c!v} \text{ for some } v \} \;\geq\; p;$$

- reduction-closed if $\mathcal{C} \mathcal{R} \mathcal{D}$ implies
  - whenever $\mathcal{C} \stackrel{\hat{\tau}}{\Longrightarrow} \Delta$, there exists Θ such that $\mathcal{D} \stackrel{\hat{\tau}}{\Longrightarrow} \Theta$ and $\Delta \ \mathcal{R}^{\circ} \ \Theta$,
  - whenever $\mathcal{D} \stackrel{\hat{\tau}}{\Longrightarrow} \Theta$, there exists Δ such that $\mathcal{C} \stackrel{\hat{\tau}}{\Longrightarrow} \Delta$ and $\Delta \ \mathcal{R}^{\circ} \ \Theta$;

Four criteria to judge equivalence, cont.

- compositional if $\mathcal{C}\mathcal{R}\mathcal{D}$ implies $(\mathcal{C}||R)\mathcal{R}(\mathcal{D}||R)$ for any process R with $qv(R)$ disjoint from $qv(\mathcal{C}) \cup qv(\mathcal{D})$,

Four criteria to judge equivalence, cont.

- compositional if $\mathcal{C}\mathcal{R}\mathcal{D}$ implies $(\mathcal{C}||R)\mathcal{R}(\mathcal{D}||R)$ for any process R with $qv(R)$ disjoint from $qv(\mathcal{C}) \cup qv(\mathcal{D})$,
- closed under super-operator application, if $\mathcal{C}\mathcal{R}\mathcal{D}$ implies $\mathcal{E}(\mathcal{C})\mathcal{R}\mathcal{E}(\mathcal{D})$ for any $\mathcal{E} \in \mathcal{SO}(\mathcal{H}_{\overline{qv(\mathcal{C})}})$.

Reduction barbed congruence

Originated in [Honda & Tokoro 1995].

Let reduction barbed congruence, written $\approx_r$, be the largest relation over configurations which is

- barb-preserving,
- reduction-closed,
- compositional,

Reduction barbed congruence

Originated in [Honda & Tokoro 1995].

Let reduction barbed congruence, written $\approx_r$, be the largest relation over configurations which is

- barb-preserving,
- reduction-closed,
- compositional,
- closed under super-operator application,
- and furthermore, if $\mathcal{C} \approx_r \mathcal{D}$ then $qv(\mathcal{C}) = qv(\mathcal{D})$ and $\mathrm{env}(\mathcal{C}) = \mathrm{env}(\mathcal{D})$.

Open bisimulation

Inspired by [Sangorigi 1996].

A relation $\mathcal{R} \subseteq \mathit{Con} \times \mathit{Con}$ is an open simulation if $\mathcal{C}\mathcal{R}\mathcal{D}$ implies that

- $qv(\mathcal{C}) = qv(\mathcal{D})$, and $\mathrm{env}(\mathcal{C}) = \mathrm{env}(\mathcal{D})$,
- for any $\mathcal{E} \in \mathcal{SO}(\mathcal{H}_{\overline{qv(\mathcal{C})}})$, whenever $\mathcal{E}(\mathcal{C}) \xrightarrow{\alpha} \Delta$, there is some Θ with $\mathcal{E}(\mathcal{D}) \stackrel{\hat{\alpha}}{\Longrightarrow} \Theta$ and $\Delta\ \mathcal{R}^\circ\ \Theta$.

A relation $\mathcal{R}$ is an open bisimulation if both $\mathcal{R}$ and $\mathcal{R}^{-1}$ are open simulations. We let $\approx_o$ be the largest open bisimulation.

Theorem : Congruence

Theorem : Congruence

- The relation $\approx_o$ between processes is preserved by all the constructors of qCCS except for summation.

Theorem : Congruence

- The relation $\approx_o$ between processes is preserved by all the constructors of qCCS except for summation.
- $\mathcal{C} \approx_o \mathcal{D}$ if and only if $\mathcal{C} \approx_r \mathcal{D}$.

Outline

Background

Preliminaries on quantum mechanics

Equivalences for quantum processes

Symbolic semantics

An algorithm for ground bisimulation

Hoare logic

Summary

An equivalence for super-operators

Let $\sqsubseteq$ be the Löwner preorder defined on operators: $A \sqsubseteq B$ if and only if $B - A$ is positive semi-definite.

For two super-operators $\mathcal{A}, \mathcal{B}$ on $\mathcal{H}$, let $\mathcal{A} \lesssim_V \mathcal{B}$ if for any $\rho \in \mathcal{D}(\mathcal{H})$, $\mathrm{tr}_{\overline{V}}(\mathcal{A}(\rho)) \sqsubseteq \mathrm{tr}_{\overline{V}}(\mathcal{B}(\rho))$, where $\overline{V}$ is the complement set of V in $qVar$.

Let $\eqsim_V$ be $\lesssim_V \cap \gtrsim_V$ and we abbreviate $\lesssim_\emptyset$ and $\eqsim_\emptyset$ to $\lesssim$ and $\eqsim$, respectively.

Super-operator valued distributions

A super-operator valued distribution Δ over S is a function from S to $\mathcal{SO}(\mathcal{H})$ such that $\sum_{s \in S} \Delta(s) \precsim \mathcal{I}_{\mathcal{H}}$.

Let $\mathcal{D}ist_{\mathcal{H}}(S)$ be the set of finite-support super-operator valued distributions over S.

Symbolic semantics

Inspired by [Hennessy & Lin 1995]

A pair of the form $(\!|t, \mathcal{E}|\!)$, where $t \in \mathcal{T}$ and $\mathcal{E} \in \mathcal{SO}_t(\mathcal{H})$, is called a snapshot. The set of snapshots is denoted by SN.

The symbolic semantics of qCCS is given by the qLTS $(SN, BAct_s, \rightarrow)$ on snapshots, where $\rightarrow \subseteq SN \times BAct_s \times \mathcal{D}ist_{\mathcal{H}}(SN)$ is the smallest relation satisfying a few rules.

Symbolic semantics

E.g.

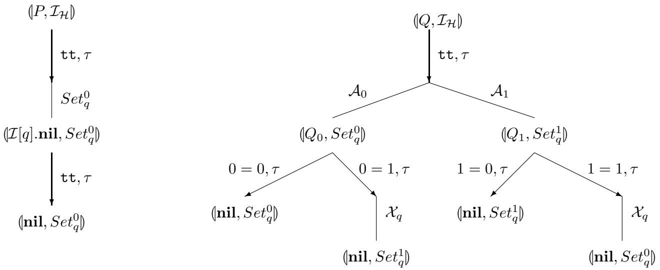
$$Meas_s \quad \frac{M = \sum_{i\in I} \lambda_i |\phi_i\rangle\langle\phi_i|}{(\!|M[\widetilde{q}; x].t, \mathcal{E}|\!) \xrightarrow{\mathtt{tt},\tau} \sum_{i\in I} \mathcal{A}_{\widetilde{r}}^{\phi_i} \bullet (\!|t\{\lambda_i/x\}, Set_{\widetilde{r}}^{\phi_i}\mathcal{E}|\!)}$$

where

$$\mathcal{A}_{\widetilde{r}}^{\phi_i} \quad : \quad \rho \mapsto |\phi_i\rangle_{\widetilde{r}}\langle\phi_i|\rho|\phi_i\rangle_{\widetilde{r}}\langle\phi_i| \tag{1}$$

$$Set_{\widetilde{r}}^{\phi_i} \quad : \quad \rho \mapsto \sum_{j\in I} |\phi_i\rangle_{\widetilde{r}}\langle\phi_j|\rho|\phi_j\rangle_{\widetilde{r}}\langle\phi_i|. \tag{2}$$

Symbolic semantics



Symbolic bisimulation

Definition

Let $\mathfrak{S} = \{\mathcal{S}^b : b \in BExp\}$ be a family of equivalence relations on SN. $\mathfrak{S}$ is called a symbolic (strong open) bisimulation if for any $b \in BExp$, $(\!|t, \mathcal{E}|\!)\mathcal{S}^b(\!|u, \mathcal{F}|\!)$ implies that

1. $qv(t) = qv(u)$ and $\mathcal{E} \eqsim_{\overline{qv(t)}} \mathcal{F}$, if b is satisfiable;
2. for any $\mathcal{G} \in \mathcal{SO}_t(\mathcal{H}_{\overline{qv(t)}})$, whenever $(\!|t, \mathcal{G}\mathcal{E}|\!) \xrightarrow{b_1,\gamma} \Delta$ with $bv(\gamma) \cap fv(b, t, u) = \emptyset$, there exists a collection of booleans B such that $b \wedge b_1 \to \bigvee B$ and $\forall\ b' \in B$, $\exists b_2, \gamma'$ with $b' \to b_2$, $\gamma =_{b'} \gamma'$, $(\!|u, \mathcal{G}\mathcal{F}|\!) \xrightarrow{b_2,\gamma'} \Xi$, and $(\mathcal{G}\mathcal{E} \bullet \Delta)\mathcal{S}^{b'}(\mathcal{G}\mathcal{F} \bullet \Xi)$.

Ground bisimulation

Definition

A family of equivalence relations $\{\mathcal{S}^b : b \in BExp\}$ is called a symbolic *ground* bisimulation if for any $b \in BExp$, $(\!|t, \mathcal{E}|\!)\mathcal{S}^b(\!|u, \mathcal{F}|\!)$ implies that

1. $qv(t) = qv(u)$ and $\mathcal{E} \approx_{\overline{qv(t)}} \mathcal{F}$, if b is satisfiable,
2. whenever $(\!|t, \mathcal{E}|\!) \stackrel{b_1,\gamma}{\rightarrow} \Delta$ with $bv(\gamma) \cap fv(b, t, u) = \emptyset$, there exists a collection of booleans B such that $b \wedge b_1 \rightarrow \bigvee B$ and $\forall\ b' \in B, \exists b_2, \gamma'$ with $b' \rightarrow b_2$, $\gamma =_{b'} \gamma'$, $(\!|u, \mathcal{F}|\!) \stackrel{b_2,\gamma'}{\rightarrow} \Xi$, and $(\mathcal{E} \bullet \Delta)\mathcal{S}^{b'}(\mathcal{F} \bullet \Xi)$.

Closure under super-operator application

Definition

A relation $\mathcal{S}$ on SN is said to be closed under super-operator application if $(\!|t, \mathcal{E}|\!)\mathcal{S}(\!|u, \mathcal{F}|\!)$ implies $(\!|t, \mathcal{G}\mathcal{E}|\!)\mathcal{S}(\!|u, \mathcal{G}\mathcal{F}|\!)$ for any $\mathcal{G} \in \mathcal{SO}_t(\mathcal{H}_{\overline{qv(t)}})$.

Theorem

A family of equivalence relations $\{\mathcal{S}^b : b \in BExp\}$ is a symbolic bisimulation if and only if it is both a ground bisimulation and closed under super-operator application.

Special case

Theorem

If t and u are both free of quantum input, then $(\!|t, \mathcal{E}|\!) \sim_s^b (\!|u, \mathcal{F}|\!)$ if and only if $(\!|t, \mathcal{E}|\!) \sim_g^b (\!|u, \mathcal{F}|\!)$.

Symbolic bisimilarity

Theorem

1. *For each* $b \in BExp$, $\sim_s^b$ *is an equivalence relation.*
2. *The family* $\{\sim_s^b : b \in BExp\}$ *is a symbolic bisimulation.*

Symbolic vs open bisimulation

Theorem

1. *$t \sim_s^b u$ if and only if for any evaluation ψ, $\psi(b) = tt$ implies $t\psi \sim_o u\psi$.*
2. *$t \sim_s u$ if and only if $t \sim_o u$.*

Outline

Background

Preliminaries on quantum mechanics

Equivalences for quantum processes

Symbolic semantics

An algorithm for ground bisimulation

Hoare logic

Summary

The algorithm

Bisim$(\mathfrak{t}, \mathfrak{u})$ = **Match**$(\mathfrak{t}, \mathfrak{u}, \mathtt{tt}, \emptyset)$

Match$(\mathfrak{t}, \mathfrak{u}, b, W) =$ where $\mathfrak{t} = (\!|t, \mathcal{E}|\!)$ and $\mathfrak{u} = (\!|u, \mathcal{F}|\!)$
if $(\mathfrak{t}, \mathfrak{u}) \in W$ **then**
  $(\theta, T) := (\mathtt{tt}, \emptyset)$
else
  for $\gamma \in Act(\mathfrak{t}, \mathfrak{u})$ **do**
    $(\theta_\gamma, T_\gamma) :=$ **MatchAction**$(\gamma, \mathfrak{t}, \mathfrak{u}, b, W)$
  end
  $(\theta, T) := (\bigwedge_\gamma \theta_\gamma, \ \bigsqcup_\gamma (T_\gamma \sqcup \{(\mathfrak{t}, \mathfrak{u}) \mapsto (b \wedge \bigwedge_\gamma \theta_\gamma)\}))$
end
return $(\theta \wedge (qv(t) = qv(u)) \wedge (\mathcal{E} \approx_{\overline{qv(t)}} \mathcal{F}), T)$

MatchAction$(\gamma, \mathfrak{t}, \mathfrak{u}, b, W) =$
...
case τ
  for $\mathfrak{t} \xrightarrow{b_i, \tau} \Delta_i$ *and* $\mathfrak{u} \xrightarrow{b'_j, \tau} \Theta_j$ **do**
    $(\theta_{ij}, T_{ij}) :=$ **MatchDistribution**$(\Delta_i, \Theta_j, b \wedge b_i \wedge b'_j, \{(\mathfrak{t}, \mathfrak{u})\} \cup W)$
  end
  return $(\bigwedge_i (b_i \rightarrow \bigvee_j (b'_j \wedge \theta_{ij})) \wedge \bigwedge_j (b'_j \rightarrow \bigvee_i (b_i \wedge \theta_{ij})), \ \bigsqcup_{ij} T_{ij})$
endsw
...

MatchDistribution(Δ, Θ, b, W)=
for $\mathfrak{t}_i \in \lceil \Delta \rceil$ *and* $\mathfrak{u}_j \in \lceil \Theta \rceil$ **do**
  $(\theta_{ij}, T_{ij}) :=$ **Match**$(\mathfrak{t}_i, \mathfrak{u}_j, b, W)$
end
$\mathcal{R} := \{(\mathfrak{t}, \mathfrak{u}) \mid b \rightarrow (\bigsqcup_{ij} T_{ij})(\mathfrak{t}, \mathfrak{u})\}^*$
return (**Check**$(\Delta, \Theta, \mathcal{R})$, $\bigsqcup_{ij} T_{ij}$)

Check$(\Delta, \Theta, \mathcal{R}) =$
$\theta := \mathtt{tt}$
for $S \in \lceil \Delta \rceil \cup \lceil \Theta \rceil / \mathcal{R}$ **do**
  $\theta := \theta \wedge (\Delta(S) \approx \Theta(S))$

Correctness

Theorem

For two snapshots $\mathfrak{t}$ *and* $\mathfrak{u}$*, the function* $\textbf{Bisim}(\mathfrak{t}, \mathfrak{u})$ *terminates.*
Moreover, if $\textbf{Bisim}(\mathfrak{t}, \mathfrak{u}) = (\theta, T)$ *then* $T(\mathfrak{t}, \mathfrak{u}) = \theta = mgb(\mathfrak{t}, \mathfrak{u})$.

Complexity

Assume the ability of real computation, the worst case time complexity of executing **Bisim**$(\mathfrak{t}, \mathfrak{u})$ is $O(n^5 / \log n)$. To implement the algorithm, we have to approximate super-operators using matrices of algebraic or even rational numbers, thus increase the complexity.

Outline

Background

Preliminaries on quantum mechanics

Equivalences for quantum processes

Symbolic semantics

An algorithm for ground bisimulation

Hoare logic

Summary

Quantum while-language [Ying 2011]

- Fix the alphabet of quantum **while**-language: A countably infinite set $qVar$ of quantum variables. Symbols $q, q', q_0, q_1, q_2, \ldots$ denote quantum variables.
- Each quantum variable $q \in qVar$ has a type $\mathcal{H}_q$ (a Hilbert space).
- For simplicity, we only consider two basic types:

$$\textbf{Boolean} = \mathcal{H}_2, \qquad \textbf{integer} = \mathcal{H}_\infty.$$

- A quantum register is a finite sequence $\overline{q} = q_1, \ldots, q_n$ of distinct quantum variables. Its state Hilbert space:

$$\mathcal{H}_{\overline{q}} = \bigotimes_{i=1}^{n} \mathcal{H}_{q_i}.$$

Quantum programs

$$
\begin{aligned}
S ::= \ & \mathbf{skip} \mid q := |0\rangle \mid \bar{q} := U[\bar{q}] \mid S_1; S_2 \\
& \mid \mathbf{if}\ (\square m \cdot M[\bar{q}] = m \rightarrow S_m)\ \mathbf{fi} \\
& \mid \mathbf{while}\ M[\bar{q}] = 1\ \mathbf{do}\ S\ \mathbf{od}.
\end{aligned}
$$

Notations

- A positive operator ρ is called a *partial density operator* if $tr(\rho) \leq 1$.
- Write $\mathcal{D}(\mathcal{H})$ for the set of partial density operators in $\mathcal{H}$.
- Write $\mathcal{H}_{all}$ for the tensor product of the state Hilbert spaces of all quantum variables:
$$\mathcal{H}_{all} = \bigotimes_{q \in qVar} \mathcal{H}_q.$$
- Let $\overline{q} = q_1, ..., q_n$ be a quantum register. An operator A in the state Hilbert space $\mathcal{H}_{\overline{q}}$ of $\overline{q}$ has a cylindrical extension $A \otimes I$ in $\mathcal{H}_{all}$.
- We will use E to denote the empty program; i.e. termination.
- A configuration is a pair $\langle S, \rho \rangle$, where:
  1. S is a quantum program or the empty program E;
  2. $\rho \in \mathcal{D}(\mathcal{H}_{all})$, denoting the (global) state of quantum variables.
- A transition between quantum configurations:

Operational semantics (selected rules)

(SC) $$\frac{\langle S_1, \rho\rangle \to \langle S_1', \rho'\rangle}{\langle S_1; S_2, \rho\rangle \to \langle S_1'; S_2, \rho'\rangle}$$

where $E; S_2 = S_2$.

(IF) $$\overline{\langle \mathbf{if}\ (\square m \cdot M[\overline{q}] = m \to S_m)\ \mathbf{fi}, \rho\rangle \to \langle S_m, M_m \rho M_m^\dagger\rangle}$$

for each possible outcome m of measurement $M = \{M_m\}$.

(L0) $$\overline{\langle \mathbf{while}\ M[\overline{q}] = 1\ \mathbf{do}\ S\ \mathbf{od}, \rho\rangle \to \langle E, M_0 \rho M_0^\dagger\rangle}$$

(L1) $$\overline{\langle \mathbf{while}\ M[\overline{q}] = 1\ \mathbf{do}\ S\ \mathbf{od}, \rho\rangle \to \langle S; \mathbf{while}\ M[\overline{q}] = 1\ \mathbf{do}\ S\ \mathbf{od}, M_1 \rho M_1^\dagger\rangle}$$

Semantic function

- Let S be a quantum program. Then its semantic function

$$[\![S]\!] : \mathcal{D}(\mathcal{H}_{all}) \to \mathcal{D}(\mathcal{H}_{all})$$

$$[\![S]\!](\rho) = \sum \{|\rho' : \langle S, \rho\rangle \to^* \langle E, \rho'\rangle|\}$$

Quantum Predicates

- What is a quantum predicate?
- A quantum predicate should be a physical observable!
- A *quantum predicate* in a Hilbert space $\mathcal{H}$ is a Hermitian operator M in $\mathcal{H}$ with all its eigenvalues lying within the unit interval $[0, 1]$.
- The set of predicates in $\mathcal{H}$ is denoted $\mathcal{P}(\mathcal{H})$.

Satisfaction of Quantum Predicates

- $tr(M\rho)$ may be interpreted as the degree to which quantum state ρ satisfies quantum predicate M.

Correctness Formulas

- A correctness formula is a statement of the form:

$$\{P\}S\{Q\}$$

  where:
  - S is a quantum program;
  - $P, Q \in \mathcal{P}(\mathcal{H}_{all})$ are quantum predicates in $\mathcal{H}_{all}$.
  - P is called the precondition, Q the postcondition.

Partial Correctness, Total Correctness

- Two interpretations of Hoare logical formula $\{P\}S\{Q\}$:
  - *Partial correctness*: If an input to program S satisfies the precondition P, then either S does not terminate, or it terminates in a state satisfying the postcondition Q.
  - *Total correctness*: If an input to program S satisfies the precondition P, then S must terminate and it terminates in a state satisfying the postcondition Q.

Partial Correctness, Total Correctness (Continued)

- The correctness formula $\{P\}S\{Q\}$ is true in the sense of *total correctness*, written

$$\models_{tot} \{P\}S\{Q\},$$

  if:

$$tr(P\rho) \leq tr(Q[\![S]\!](\rho))$$

  for all $\rho \in \mathcal{D}(\mathcal{H}_{all})$, where $[\![S]\!]$ is the semantic function of S.

- The correctness formula $\{P\}S\{Q\}$ is true in the sense of *partial correctness*, written

$$\models_{par} \{P\}S\{Q\},$$

  if:

$$tr(P\rho) \leq tr(Q[\![S]\!](\rho)) + [tr(\rho) - tr([\![S]\!](\rho))]$$

  for all $\rho \in \mathcal{D}(\mathcal{H}_{all})$.

Hoare logic for partial correctness (selected rules)

(R – SC) $$\frac{\{P\}S_1\{Q\} \quad \{Q\}S_2\{R\}}{\{P\}S_1;S_2\{R\}}$$

(R – IF) $$\frac{\{P_m\}S_m\{Q\} \text{ for all } m}{\{\sum_m M_m^\dagger P_m M_m\}\ \textbf{if}\ (\square m \cdot M[\overline{q}] = m \rightarrow S_m)\ \textbf{fi}\{Q\}}$$

(R – LP) $$\frac{\{Q\}S\,\{M_0^\dagger P M_0 + M_1^\dagger Q M_1\}}{\{M_0^\dagger P M_0 + M_1^\dagger Q M_1\}\textbf{while}\ M[\overline{q}] = 1\ \textbf{do}\ S\ \textbf{od}\{P\}}$$

(R – Or) $$\frac{P \sqsubseteq P' \quad \{P'\}S\{Q'\} \quad Q' \sqsubseteq Q}{\{P\}S\{Q\}}$$

Soundness Theorem

For any quantum **while**-program S and quantum predicates $P, Q \in \mathcal{P}(\mathcal{H}_{all})$:

$$\vdash_{qPD} \{P\}S\{Q\} \text{ implies } \models_{par} \{P\}S\{Q\}.$$

(Relative) Completeness Theorem

For any quantum **while**-program S and quantum predicates $P, Q \in \mathcal{P}(\mathcal{H}_{all})$:

$$\models_{par} \{P\}S\{Q\} \text{ implies } \vdash_{qPD} \{P\}S\{Q\}.$$

Theorem prover for quantum programs

- A theorem prover for quantum Hoare logic based on Isabelle/HOL has been implemented by Liu et al.

Theorem prover for quantum programs

- A theorem prover for quantum Hoare logic based on Isabelle/HOL has been implemented by Liu et al.
- `https://arxiv.org/pdf/1601.03835.pdf`

Outline

Background

Preliminaries on quantum mechanics

Equivalences for quantum processes

Symbolic semantics

An algorithm for ground bisimulation

Hoare logic

Summary

Summary

- A natural extensional behavioural equivalence between quantum processes.

Summary

- A natural extensional behavioural equivalence between quantum processes.
- An open bisimulation to provide a sound and complete proof methodology.

Summary

- A natural extensional behavioural equivalence between quantum processes.
- An open bisimulation to provide a sound and complete proof methodology.
- Symbolic semantics

Summary

- A natural extensional behavioural equivalence between quantum processes.
- An open bisimulation to provide a sound and complete proof methodology.
- Symbolic semantics
- An algorithm for ground bisimulation

Summary

- A natural extensional behavioural equivalence between quantum processes.
- An open bisimulation to provide a sound and complete proof methodology.
- Symbolic semantics
- An algorithm for ground bisimulation
- Hoare logic for quantum programs

Future work

Future work

- Symbolic weak bisimulation?

Future work

- Symbolic weak bisimulation?
- Apply the open bisimulation to analyze quantum cryptographic protocols, e.g. BB84 quantum key distribution protocol

Future work

- Symbolic weak bisimulation?
- Apply the open bisimulation to analyze quantum cryptographic protocols, e.g. BB84 quantum key distribution protocol
- Model checking for quantum protocols

Future work

- Symbolic weak bisimulation?
- Apply the open bisimulation to analyze quantum cryptographic protocols, e.g. BB84 quantum key distribution protocol
- Model checking for quantum protocols
- Termination analysis

Future work

- Symbolic weak bisimulation?
- Apply the open bisimulation to analyze quantum cryptographic protocols, e.g. BB84 quantum key distribution protocol
- Model checking for quantum protocols
- Termination analysis
- Invariant generation

Future work

- Symbolic weak bisimulation?
- Apply the open bisimulation to analyze quantum cryptographic protocols, e.g. BB84 quantum key distribution protocol
- Model checking for quantum protocols
- Termination analysis
- Invariant generation
- Fully abstract denotational semantics

(Incomplete) references

1. M. S. Ying, Foundations of Quantum Programming, Elsevier - Morgan Kaufmann, 2016.
2. A. S. Green, P. L. Lumsdaine, N. J. Ross, P. Selinger and B. Valiron, Quipper: A scalable quantum programming language, Proc. PLDI 2013, pp. 333-342.
3. D. Wecker and K. M. Svore, LIQUi$|\ >$: A software design architecture and domain-specific language for quantum computing, `http://research.microsoft.com/pubs/209634/1402.4467.pdf`.
4. A. J. Abhari, A. Faruque, M. Dousti, L. Svec, O. Catu, A. Chakrabati, C.-F. Chiang, S. Vanderwilt, J. Black, F. Chong, M. Martonosi, M. Suchara, K. Brown, M. Pedram and T.Brun, Scaffold: Quantum Programming Language, Technical Report TR-934-12, Dept. of Computer Science, Princeton University, 2012.
5. M. Pagani, P. Selinger and B. Valiron, Applying quantitative semantics to higher-order quantum computing, Proc. POPL 2014, pp. 647-658.
6. E. D'Hondt and P. Panangaden, Quantum weakest preconditions, Mathematical Structures in Computer Science, 16(2006)429-451.

7. P. Jorrand and M. Lalire, Toward a quantum process algebra, Proceedings of the 1st ACM Conference on Computing Frontier, 2004, pp. 111-119.
8. S. J. Gay and R. Nagarajan, Communicating Quantum Processes, Proc. POPL 2005, pp. 145-157.
9. Y. Feng, R. Y. Duan and M. S. Ying, Bisimulation for quantum processes, Proc. POPL 2011, pp. 523-534.
10. Y. Deng and Y. Feng. Open Bisimulation for Quantum Processes. In Proc. IFIP TCS 2012. LNCS 7604, pp. 119-133. Springer, 2012.
11. Y. Feng, Y. Deng, and M. Ying. Symbolic bisimulation for quantum processes. ACM Transactions on Computational Logic, Vol. 15, No. 2, Article 14, April 2014.

Thank you!